CyOTE CASE STUDY: TRITON IN PETRO RABIGH

SEPTEMBER 23, 2021

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL Idaho National Laboratory

Table of Contents

CYOTE CASE STUDY: TRITON IN PETRO RABIGH

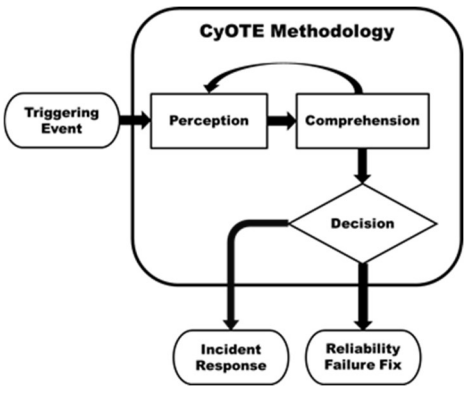
INTRODUCTION

The CyOTE methodology developed capabilities for energy sector asset owners and operators (AOOs) to independently identify adversarial tactics, techniques, and procedures (TTPs) within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE), CyOTE is a partnership with energy sector owners and operators. CyOTE seeks to tie effects of a cyber-attack to anomalies—as detected by commercial or in-house solutions—in the OT environment to determine if it has a malicious cyber cause.

Case Studies support continued learning through analysis of incidents and events. Some of the richest and most detailed Case Studies are expected to be produced by AOOs who have employed the CyOTE methodology to perceive and comprehend actual triggering events in their OT environments, with the benefit of complete access to all data and full context. To bootstrap the learning process and complement anticipated AOO-generated Case Studies, the CyOTE team has begun compiling Case Studies of historical OT attacks and OT-related incidents.

This historical Case Study is based on publicly available reports of the incident from media outlets and cybersecurity firms instead of the full context and data that an AOO would have. This Case Study is not, nor is it intended to be, completely comparable in detail or structure, nonetheless it provides examples of how key concepts in CyOTE methodology look in the real world. Perhaps more importantly, evaluating this historical incident through the CyOTE methodology provides a learning opportunity from the perspective of "how could this have been detected?" instead of "why was this missed?" to grow the body of knowledge on perception, comprehension, and organizational capabilities.

METHODOLOGY



The CyOTE methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. MITRE's ATT&CK® Framework for Industrial Control Systems (ICS)[1] is used as a common lexicon to identify a set of triggering events related to three Use Cases – Alarm Logs, Human-Machine Interface (HMI), and Remote Logins – which together account for 87 percent of the techniques commonly used by adversaries. The CyOTE methodology is also appropriate for OT-related anomalies perceived outside the three Use Cases, such as through the energy system itself.

The Case Study highlights the CyOTE methodology for an AOO to use, starting from the point in time and space an anomalous event or condition meriting investigation – a triggering event – is perceived, and continues to the point where the anomaly is comprehended with sufficient

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

confidence to make a business risk decision on the appropriate resolution. If sufficient evidence of a malicious nexus is found, then the situation is addressed through existing organizational incident response procedures. Failure to find sufficient evidence of malicious activity defaults to the situation addressed through existing organizational corrective maintenance and work management procedures.

By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables which could represent a faint signal of an attack requiring investigation. CyOTE can assist AOOs in prioritizing their OT environment visibility investments. Over time, AOOs' triggering events will move towards fainter signals, detected earlier, to interdict incidents before more significant harms are realized in the face of infrastructure changes, new technologies, and determined and sophisticated adversaries.

BACKGROUND ON THE ATTACK

In June 2017, a section of the Petro Rabigh refinery complex in Rabigh, Saudi Arabia shut down as a result of a Safety Instrumented System (SIS) controller entering a failed "safe state." Since there was no apparent reason for the shutdown, the AOO conducted further analysis.[2] Testing and analysis of a "glitchy" Triconex SIS controller was conducted onsite and in a California laboratory. These analyses drove a review of logs from the plant, and determined the failure was mechanical in nature.

The same incident reoccurred in August 2017, again causing operations disruptions. This prompted engineers to conduct a more thorough causal analysis. Identification of unusual communications beaconing between the complex's IT environment and engineering workstations located in the OT environment were the key to uncovering an ongoing cyber campaign targeting the complex's Triconex SIS controllers.[3]

The triggering event for this incident was the second occurrence of the controller entering a failed "safe state." Subsequent to investigation of the second instance of a shutdown of a section of the plant with an SIS controller in a failed state, the discovery of unusual network traffic between the complex's IT environment and engineering workstations in the OT environment was also discovered. This apparent beaconing traffic was the revelation that changed the effort from an investigation of a repeat equipment failure to an investigation of a security concern.

MAP OF ATTACK TTPS

By mapping the techniques, tactics, and procedures an attacker used to gain access, CyOTE researchers examine where greater monitoring and detection could provide the visibility needed to connect the dots on attacker activity. The Petro Rabigh incident involved the use of adversary techniques from all three CyOTE Use Cases – Alarm Logs, Remote Login and Human Machine Interface. Nineteen techniques across six series-parallel steps were eventually identified as part of this complex and protracted attack campaign. These techniques, in chronological sequence as employed by the adversary and not in order of detection by the victim, are shown in Figure 1.

[2] https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware
[3] https://www.eenews.net/stories/1060123327

AOOs can utilize this information in their own environments to quickly identify potential attacks and take mitigative actions.

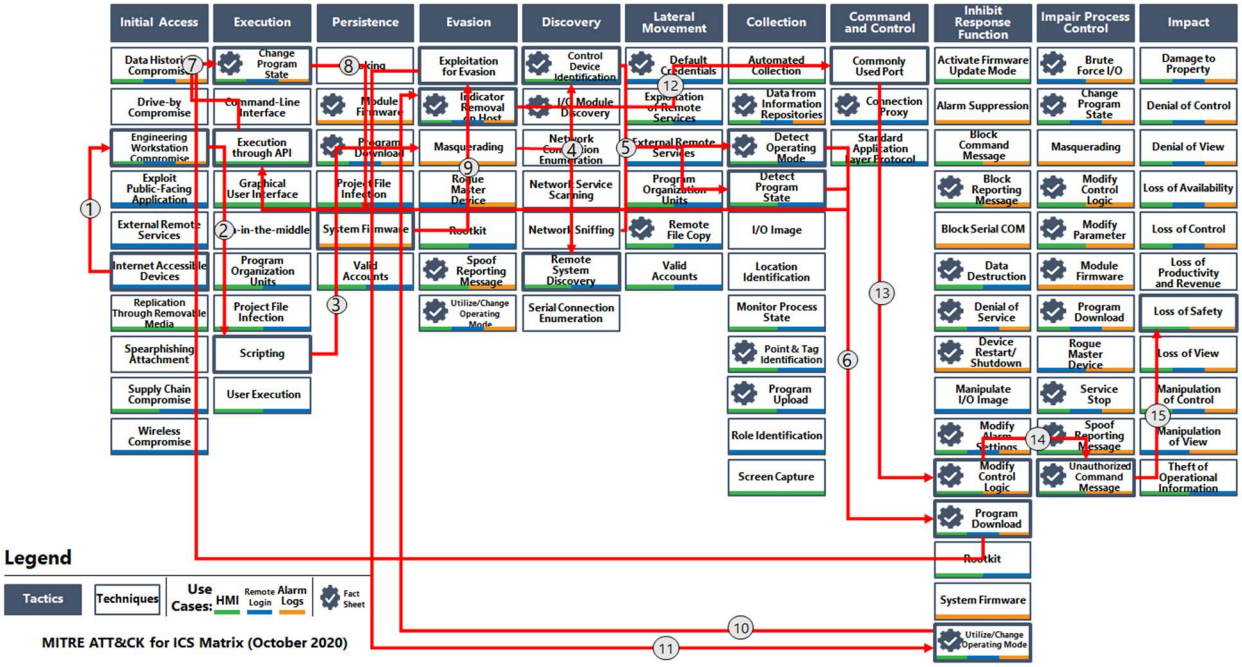


Figure 1. Petro Rabigh Incident Adversary Techniques Chain

Anomalies, possible related adversary techniques, and example perception methods for the anomalies, broken down by general adversary campaign steps, are detailed below.

APPLICATION OF CyOTE METHODOLOGY AND TECHNIQUES TO THE ATTACK PATH

IT Network Exploitation

Anomalies:

- Increased demilitarized zone (DMZ) traffic between IT and OT networks and beaconing coming from the control network. This anomaly was the triggering event in this Case Study.
- Anti-virus software alerted to the presence of the MIMIKATZ credential harvesting tool, in the IT network.[4]
- Employee phone numbers modified from expected numbers.

Technique: Internet Accessible Device – Remote attackers gained access to corporate computers through a poorly configured firewall, then pivoted to OT networks.

[4]https://www.darkreading.com/attacks-breaches/triton-trisis-attack-was-more-widespread-than-publicly-known/d/d-id/1333661

Perception Opportunities:

- Investigating identified attacks against IT assets for potential to traverse networks.
- Verifying modifications to important employee information.
- Monitoring traffic between networks.
- Assessing new or unusual connections such as Remote Desktop Protocol sessions.

Move to OT Network

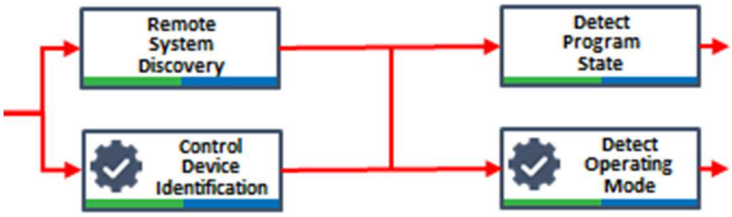
Anomaly: Unfamiliar Py2exe compiled binaries present in an OT environment.

Techniques:

- Engineering Workstation Compromise – "The attacker gained remote access to an SIS engineering workstation and deployed the TRITON attack framework to reprogram the SIS controllers...The malware was delivered as a Py2exe compiled python script dependent on a zip file containing standard Python libraries, open-source libraries, as well as the attacker-developed Triconex attack framework for interacting with the Triconex controllers."[5]
- Masquerading – The name of the Triton malware, "trilog.exe", mimicked the legitimate Triconex Trilog application.

Perception Opportunities: Periodic endpoint scans for unexpected or inappropriate file types or locations.

OT Attack Capability Development



Anomaly: IP addresses for Triconex SIS were discovered in malware code.

Techniques:

- Control Device Identification
- Remote System Discovery

The malware on the engineering workstation contained the ability to send a UDP broadcast packet to identify Triconex devices on the network. This functionality was not used, however, and the IP addresses for the Triconex devices were input directly indicating the adversaries had already obtained the IP addresses.

[5] https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html

CyOTE Proof of Concept Tool: The CyOTE T808 Control Device Identification Proof of Concept tool could have logged the use of network traffic which can be used to fingerprint or identify a control device. This capability could be leveraged by the AOO to support the Triconex protocol and the broadcast packets used in this attack. The AOO could use the Control Device Identification tool to monitor supported devices and protocols through either live (via a span port) or recorded (via PCAP files) network traffic. The Proof of Concept tool allows an AOO to define a list of hosts allowed to communicate with a device, such as an engineering workstation.

Techniques:

- Detect Operating Mode
- Detect Program State

The script contained a function which collected key and operating states, and other project information.[6]

CyOTE Proof of Concept Tool: The CyOTE T868 Detect Operating Mode Proof of Concept tool could have been used to perform deep packet inspection of Modbus protocols to alert when a "read register" command is identified for the operating mode register. An "allow/deny" configuration file is used to filter alerts from approved hosts and flag unapproved host commands. This capability could be leveraged by an AOO to support the Triconex protocol and command used to detect the operating mode of the device.

OT Attack Capability Delivery

Anomaly: Unexpected shellcode was present on six Triconix SIS controllers.[7]

Techniques:

- Execution through API
- Program Download
- Change Program State

A script used the TriStation protocol for program download, allocation, and modifications. The program was transferred to the Triconex device multiple times overwriting with an empty program checking and then overwriting with the malicious program.

- System Firmware – Shellcode containing two parts, one for running on the system and another for command and control, was injected.

CyOTE Recipe: The CyOTE T843 Program Download Recipe could be used to guide an AOO through the development of a network monitoring capability to detect traffic

[6] https://github.com/MDudek-ICS/TRISIS-TRITON-HATMAN/blob/master/decompiled_code/library/TsHi.py
[7] https://www.darpa.mil/news-events/2021-02-23.

which would download a device's program. The current capability outlines the process an AOO should consider when building a tool to analyze the OT network traffic and through deep packet inspection to identify potential indicators arising from an attempt to download the program.

CyOTE Recipe: The CyOTE T875 Change Program State Recipe could be used to guide an AOO through development of a capability to read and analyze network traffic captures based upon set criteria, located in a separate configuration file. The criteria compare protocol layer fields to static values (e.g., MAC and statically defined IP addresses of hosts). The Recipe identifies the need to alert on trusted IP lists for unauthorized traffic detection, monitors for PLC program download commands from unauthorized host(s), and controllers' running programs forced to a new state (e.g., reset, start, halt) from an operator or engineering workstation.

Supporting Attack – Hide

Techniques:

- Exploitation for Evasion – Triton malware disables RAM/ROM consistency checking.
- Utilize/Change Operating Mode – Triton malware only affects controllers left in "Program Mode." Once installed, however, it modifies the system to allow code to ignore key-switch position.
- Indicator Removal on Host – Triton malware attempts to reset the controller to a previous state. If this failed, it would write a dummy program overwriting the malicious program.
- Commonly Used Port – The malware communicates with the implant on the Triconex device using specifically crafted legitimate network packets.

CyOTE Recipe: The T872 Indicator Removal on Host Recipe could provide an AOO with industry standard remote process monitoring, remote log aggregation, and best practice host-based access control configuration. The Recipe identifies remote process and log monitoring via a SYSLOG messaging service or a host-based agent, depending on the host's capabilities. The Recipe highlights the data collected and analysis using Elasticsearch and potential alerts resulting from finding indicators of compromise using Kibana messaging.

OT Attack Execution and Impact

Anomaly: A portion of the plant shut down with the SIS controller in a failed state.

Technique:

- Modify Control Logic – The malware can reprogram the SIS logic of the Triconex device to trip or shutdown while in a safe state, or conversely to not trip and continue running to allow unsafe conditions to persist.
- Unauthorized Command Message – An adversary can manipulate the process into an unsafe state from the DCS while preventing the SIS from functioning appropriately.

- Loss of Safety – The malware has the capability to reprogram SIS logic allowing unsafe conditions to persist or to allow an unsafe state while using the distributed control system (DCS) to create an unsafe state or hazard.

CyOTE Recipe: The CyOTE T833 Modify Control Logic Recipe could guide an AOO on analyzing OT network traffic and uses deep packet inspection to identify potential indicators arising from an attempt to modify control logic.

CyOTE Proof of Concept Tool: The CyOTE T855 Unauthorized Command Message Proof of Concept tool could be used to read a network traffic capture and analyze it based upon a set of criteria defined in a separate configuration file. The criteria compare the protocol layer fields to static values, alerting on trusted IP lists for unauthorized traffic detection, and validating the CIP protocol. The tool output provides statistics about triggered criteria, such as number of times triggered, which packets caused the trigger, data about the network streams, and which network streams included the full protocol cycle or only a part. The protocol validation summary also identifies the packets associated with validation (or lack thereof).

Decision: Petro Rabigh's leadership decided this situation was a cybersecurity incident and initiated their response procedures. Without the firsthand knowledge and records an AOO would have, the specific point in time this decision was reached is not known, but generally understood to be shortly after the perception of the triggering event.

CONCLUSION

The Triton Case Study emphasizes how the CyOTE methodology can be utilized by AOOs, even at different maturity levels, to detect indicators of attack earlier along a complex attack chain. Using the CyOTE methodology, an AOO can filter signal from noise to identify interconnected anomalies, trigger further investigation, and escalate response procedures. AOOs can utilize commercial tools and/or CyOTE capabilities to increase visibility and comprehension across the three CyOTE Use Cases. Deeper comprehension will allow AOOs to successfully identify and comprehend indicators of attack earlier in the campaign in order to respond to and resolve incidents with ever decreasing impacts. Furthermore, deeper comprehension of the OT environment allows AOOs sufficient confidence to make risk-informed decisions on whether to declare a cybersecurity incident and begin response procedures in the OT environment when anomalies occur outside the OT environment.

SCENARIO CONSIDERATIONS

After reviewing this Case Study, AOOs should consider how a similar scenario could unfold in their operating environment, determine the level and location of visibility necessary for them to perceive the triggering event and other anomalies, and identify accessible information sources to build comprehension. The following questions for reflection and discussion can help AOOs prepare to employ the CyOTE Methodology in their organization.

- Could you perceive a similar triggering event in your organization? How would it be perceived, and by whom?

- What observables exist that could have been perceived earlier than the triggering event was? How would each be perceived, and by whom?
- Who will you contact from the System Operations, Engineering, and Cybersecurity departments to build comprehension? Would they be willing and able to assist today?
- How much evidence would you need to confidently reject the null hypothesis of a reliability failure, and initiate cybersecurity incident response procedures?
- Who else in your organization needs to be aware of the outcome?

AOOs can refer to the CyOTE methodology for more information on CyOTE's approach to identifying anomalies in an OT environment, which, when perceived, initiates investigation and analysis to comprehend the anomaly.

Click for More Information	CyOTE Program || Fact Sheet || CyOTE.Program@hq.doe.gov
DOE Senior Technical Advisor	Edward Rhyne || Edward.Rhyne@hq.doe.gov || 202-586-3557